UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,479	12/04/2003	Mark Kraus	223816	6237

22801 7590 04/05/2007
LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	04/05/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 04/05/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/727,479	KRAUS ET AL.	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 12/4/03 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Thanhnga B. Do
AU2135

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-34 have been examined and are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 23-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Cromer, et al. (US 6,684,326).

As per claim 23:

A portable computing device, comprising:

flash memory, the flash memory including a protected area and an unprotected a bootloader stored in the protected area of flash memory, the bootloader containing a crypto module; **(col.4, lines 17-57)**

an operating system image stored in the unprotected area of flash memory; **(col.3, lines 23-27)**

random access memory (RAM); and **(col.11, lines 31-35)**

wherein the crypto module of the bootloader is operative to examine an image update to determine if the image update should be programmed into the unprotected area of flash memory to boot the device based on information included in a signed catalog file embedded in the image update. **(col.5, lines 8-14 and 36-62)**

As per claim 24: see Cromer on col.3, lines 22-26; discussing device of claim 23, wherein the crypto module programs the image update into the unprotected area of flash memory when the device is in test mode.

As per claim 25: see Cromer on col.3, lines 22-26 and col.5, lines 17-35; discussing device of claim 23, wherein the bootloader stores the image update in the RAM until the crypto module determines that the image update should be programmed into the unprotected area of flash memory to boot the device.

As per claim 26: see Cromer on col.5, lines 38-62; discussing device of claim 25, wherein the crypto module calculates a first hash of the image update, extracts a second hash from the catalog file, and compares the first hash and the second hash, the crypto module blocking use of the image update when the first hash and the second hash do not match.

As per claim 27: see Cromer on col.1, lines 53-57 and col.5, lines 11-67; discussing device of claim 25, wherein the crypto module extracts a signature certification from the catalog file and attempts to validate the signature certification, the

crypto module blocking use of the image update when the signature certification cannot be validated.

As per claim 28: see Cromer on col.5, lines 12-14 and 38-62; discussing device of claim 25, wherein the crypto module extracts make and model attributes from the catalog file and compares them to make and model information for the device, the crypto module blocking use of the image update when the make and model attributes of the image update do not match the make and model attributes of the device.

As per claim 29: see Cromer on col.3, lines 22-26; discussing device of claim 25, wherein the bootloader erases a current device image from the unprotected area of flash memory and programs the image update into the unprotected area of flash memory when the crypto modules determines that the image update may be used to boot the device.

As per claim 30: see Cromer on col.1, lines 53-57 and col.5, lines 12-14 and 38-62; discussing device of claim 23, wherein a second crypto module of a Mira shell is operative upon a reset of the device to examine the installed operating system image to determine if the installed operating system image should be used to boot the device based on information included in a signed catalog file embedded in the installed operating system image.

As per claim 31: see Cromer on col.5, lines 55-67; discussing device of claim 30, wherein the crypto module in the Mira shell calculates a first hash of the install operating system image, extracts a second hash from the catalog file, and compares the first hash

and the second hash, the crypto module in the Mira shell blocking use of the image update when the first hash and the second hash do not match.

As per claim 32: see Cromer col.1, lines 53-57 and col.5, lines 11-14 and 55-67; discussing device of claim 30, wherein the crypto module in the Mira shell extracts a signature certification from the catalog file and attempts to validate the signature certification, the crypto module in the Mira shell blocking use of the installed operating system image when the signature certification cannot be validated.

As per claim 33: see Cromer on col.5, lines 27-55; discussing device of claim 30, wherein the crypto module in the Mira shell extracts make and model attributes from the catalog file and compares them to make and model information for the device, the crypto module in the Mira shell blocking use of the installed operating system image when the make and model attributes of the installed operating system image do not match the make and model attributes of the device.

As per claim 34: see Cromer on col.5, lines 15-26; discussing device of claim 30, wherein the crypto module in the Mira shell allows the installed operating system image to be used to boot the device when the device is in test mode.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanderpool, et al. (US 5,781,773), and further in view of Cromer, et al. (US 6,684,326).

As per claim 1:

A method of file system protection for a resource-sparing operating system (OS) image, comprising the steps of:

loading the image into random access memory (RAM), the image including a catalog file embedded therein; **(col.11, lines 31-35)**

creating a first hash of the image; **(col.8, lines 5-15)**

extracting a second hash of the image from the catalog file; and **(col.7, line 63 – col.8, line 40)**

The catalog file can broadly interpret as a list containing specific information (i.e. name, location, or hash algorithm). Vanderpool discloses digital audio and compressed video (image) may also be linked to the data record by listing number and copied to and stored in the subdirectories under a hash algorithm as a function of the listing number.

Vanderpool discloses listing or directories of hash algorithms corresponding to a thumbnail image and its filenames reads on the claimed hash of the image from the catalog file. (col.7, line 63 – col.8, line 40). Vanderpool includes hashing of the images extracting a second hash of the image from the catalog file, but did not go further in details of a comparison/matching process. Thus, Vanderpool did not include blocking the use of the image to boot the computing device when the first hash and the second hash do not match.

Cromer disclose a method and system for performing an authenticated boot of a computer system wherein the boot process for a computer system attached to a network is authenticated to ensure authorized access to an operating system image (col.1, lines 48-51 and col.5, lines 63-65). Cromer disclose a pre specified list of bootable devices is presented to the user for selection and a determination of the selected device whether it contains an image of a desired operating system (col.5, lines 22-35). Comer discusses hashing the boot record with a hash algorithm and determines if the system boots approves or not whereby a password is requested if the boot records are not approved. Thereafter, if the password is invalid, then the system is halted (col.5, lines 40-47). Further, Cromer discloses comparing the decrypted received hash to a list of authorized operating system boot record hashes (col.5, lines 55-56). Based on the whether the received hash matches an authorized hash, the system then boots or halts appropriately (col.5, lines 59-62). The list of authorized operating system boot record hashes is obviously the claimed second hash of the image from the catalog file because as established earlier, the catalog file is merely a listing of specific

information. This reads on the claimed second hash of the image from the catalog file and blocking the use of the image to boot the computing device when the first hash and the second hash do not match.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Vanderpool with the teach of blocking the use of the image to boot the computing device when the first hash and the second hash do not match as taught by Cromer because this ensures the boot process for a computer system is authenticated to ensure authorized access to an operating system image which avoids booting an incorrect operating system image (col.5, lines 55-67).

As per claim 2: **see Cromer on col.5, lines 55-67;** discussing the method of claim 1, wherein the step of blocking the use of the image to boot the computing device when the first hash and the second hash do not match comprises the step of determining an operational mode of the computing device is set to a run mode of operation.

As per claim 3: **see Cromer on col.3, lines 22-26 and col.5, lines 15-18;** discussing method of claim 2, wherein the step of blocking the use of the image to boot the computing device when the first hash and the second hash do not match is bypassed when the step of determining the operational mode of the computing device is set to a test mode of operation, the method further comprising the step of loading the image into a flash memory of the computing device.

As per claim 4: **see Cromer on col.1, lines 53-57 and col.5, lines 11-67;**

discussing method of claim 1, further comprising the steps of validating a signature certification of the catalog file, and blocking the use of the image to boot the computing device when the signature certification of the catalog file cannot be validated.

As per claim 5: **see Cromer on col.1, lines 53-57 and col.5, lines 11-67;** discussing method of claim 4, wherein the step of blocking the use of the image to boot the computing device when the signature certification of the catalog file cannot be validated comprises the step of determining an operational mode of the computing device is set to a run mode of operation.

As per claim 6: **see Cromer on col.1, lines 50-52 and col.3, lines 22-26;** discussing method of claim 5, wherein the step of blocking the use of the image to boot the computing device when the signature certification of the catalog file cannot be validated is bypassed when the step of determining the operational mode of the computing device is set to a test mode of operation, the method further comprising the step of loading the image into a flash memory of the computing device.

As per claim 7: **see Cromer on col.5, lines 55-67;** discussing method of claim 1, further comprising the steps of extracting first make and model attributes from the catalog file, comparing the first make and model attributes from the catalog file with second make and model attributes of the computing device, and blocking the use of the image to boot the computing device when the first make and model attributes do not match the second make and model attributes.

As per claim 8: **see Cromer on col.5, lines 55-67;** discussing method of claim 7, wherein the step of blocking the use of the image to boot the computing device when

the first make and model attributes do not match the second make and model attributes comprises the step of determining an operational mode of the computing device is set to a run mode of operation.

As per claim 9: **see Cromer on col.1, lines 50-52 and col.3, lines 22-26 and col.5, lines 15-18;** discussing method of claim 8, wherein the step of blocking the use of the image to boot the computing device when the first make and model attributes do not match the second make and model attributes is bypassed when the step of determining the operational mode of the computing device is set to a test mode of operation, the method further comprising the step of loading the image into a flash memory of the computing device.

As per claim 10: **see Cromer on col.3, lines 22-26;** discussing method of claim 1, further comprising the step of booting the computing device from a prior image already loaded in flash memory of the computing device.

As per claim 11:

A method of file system protection for a resource-sparing operating system (OS) image, the image including a catalog file embedded therein, comprising the steps of:

examining the catalog file and the image to determine if the image is a properly released image; and

blocking use of the image to boot the computing device when the step of examining determines that the image is not a properly released image.

As per claim 12: **see Cromer on col.11, lines 31-35;** discussing method of claim 11, wherein the step of examining is initiated upon a request to update the image, the

method further including the step of loading an update image into random access memory (RAM).

As per claim 13: **see Cromer on col.5, lines 15-18;** discussing method of claim 1 l, wherein the step of examining is initiated upon a reset of the device.

As per claim 14: **see Cromer on col.5, lines 55-67;** discussing method of claim 11, wherein the step of examining comprises the steps of: creating a first hash of the image; extracting a second hash of the image from the catalog file; and comparing the first hash and the second hash, and wherein a mismatch provides an indication that the image is not a properly released image.

As per claim 15: **see Cromer on col.5, lines 15-67;** discussing method of claim 14, further comprising the step of determining an operational mode of the device, and wherein the step of blocking the use of the image to boot the device is bypassed when the operational mode is set to test mode.

As per claim 16: **see Cromer on col.1, lines 53-57 and col.5, lines 11-67;** discussing the method of claim 11, wherein the step of examining comprises the steps of: extracting a signature certification from the catalog file; validating the signature certification; and wherein failure of the step of validating the signature certification provides an indication that the image is not a properly released image.

As per claim 17: **see Cromer on col.5, lines 55-67;** discussing method of claim 16, further comprising the step of determining an operational mode of the device, and wherein the step of blocking the use of the image to boot the device is bypassed when the operational mode is set to test mode.

As per claim 18: see Cromer on col.5, lines 22-35 and 55-67; discussing the method of claim 11, wherein the step of examining comprises the steps of: extracting first make and model attributes from the catalog file; comparing first make and model attributes from the catalog file to second make and model attributes of the device; and wherein a mismatch between the first and the second make and model attributes provides an indication that the image is not a properly released image for the device.

As per claim 19: see Cromer on col.5, lines 15-35; discussing method of claim 18, further comprising the step of determining an operational mode of the device, and wherein the step of blocking the use of the image to boot the device is bypassed when the operational mode is set to test mode.

As per claim 20: see Vanderpool on col.11, lines 31-36; discussing method of claim 11, further comprising the step of loading the image into random access memory (RAM) of the device, and wherein the step of examining is processed after the step of loading.

As per claim 21: see Cromer on col.3, lines 22-26 and 60-62; discussing method of claim 11, wherein when the step of examining determines that the image is a properly released image, the method further comprising the steps of: erasing a previous image from flash memory of the device; programming the flash memory of the device with the properly released image.

As per claim 22: See Cromer on col.1, lines 53-57 and col.5, lines 11-67; discussing the method of claim 11, wherein the step of examining comprises the steps of: creating a first hash of the image; extracting a second hash of the image from the

catalog file; comparing the first hash and the second hash; extracting a signature certification from the catalog file; validating the signature certification; and extracting first make and model attributes from the catalog file; comparing first make and model attributes from the catalog file to second make and model attributes of the device; and wherein any one of a first mismatch between the first hash and the second hash, a failure of the step of validating the signature certification, and a second mismatch between the first and the second make and model attributes provides an indication that the image is not a properly released image for the device.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Thanhnga B. Do
AU2135

LHa